The Honorable John C. Coughenour

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

REBECCA COUSINEAU, individually on her own behalf and on behalf of all others similarly situated, Plaintiff, v. MICROSOFT CORPORATION, a Delaware corporation, Defendant.	No. 11-cv-01438-JCC MICROSOFT'S REPLY IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT ***Note on Motion Calendar:*** January 17, 2014 **Oral Argument Requested**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

Federal Statutes

Other Authorities

I. INTRODUCTION

The Stored Communications Act ("SCA") protects against "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." S. Rep. No. 541, 99th Cong., 2nd Sess. 1986, 1986 U.S.C.C.A.N. 3555, 3589, 1986 WL 31929, *35 (Oct. 17, 1986). Microsoft did none of this. It never accessed data (much less communications) in random access memory ("RAM") on Ms. Cousineau's phone—indeed, it ***cannot*** do so. Ms. Cousineau, however, complains because a Windows Phone 7 software component (i.e., the Camera app) without her permission accessed location tiles in RAM. The behavior occurred entirely on her phone, without transmitting any data to Microsoft—or anyone else. The software's behavior had no effect on Ms. Cousineau's privacy, and it gave no advantage to Microsoft, which had no way even to know the software accessed RAM. Despite this, Ms. Cousineau seeks statutory damages against Microsoft under the SCA.

On this record, the Court should grant summary judgment for any one of four reasons:

First, Ms. Cousineau admits Microsoft itself never accessed information in RAM, and she cannot articulate an intelligible theory under which the SCA would impose liability on a software developer simply because ***software*** unexpectedly accesses data—without anyone other than the user accessing an electronic communication. Because the Camera application's call to RAM did not allow Microsoft to access any electronic communication, it faces no liability under the SCA.

Second, Ms. Cousineau admits she "authorized Microsoft to access her location information on discrete occasions" and limits her SCA claim to an argument Microsoft exceeded its authorization. But "exceed[ing] authorized access" under the SCA means accessing communications the defendant has no right to access ***at all***. Because Ms. Cousineau concedes Microsoft had the right to access tiles in RAM in some circumstances, she has no SCA claim.

Third, Ms. Cousineau concedes the most recent cases uniformly hold a smartphone fails to qualify as a "facility through which an electronic communications service is provided," 18 U.S.C. § 2701(a), as required for SCA liability. Although Ms. Cousineau argues smartphones qualify as facilities providing location services, this Court reserved final decision on the issue, and the only case to decide it holds the opposite. *See In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012). Further, if smartphones were facilities, location service providers such as Microsoft (not just users such as Ms. Cousineau) would have the right to authorize third-party access to the devices, an illogical result Congress clearly did not intend—as many courts hold.

Fourth, SCA liability arises only from unauthorized access to communications temporarily stored while in transit from sender to recipient. But the tiles in RAM are not in transit between sender and recipient—they have arrived at their destination and never leave the device.

II. FACTUAL BACKGROUND

Ms. Cousineau no longer argues Microsoft collected location data from her Windows Phone 7 device without her consent or ever "tracked" her at all—even though her complaints hinged on those now-discredited allegations. *See, e.g.*, 3rd Am. Compl. [Dkt. 64] ¶¶ 1, 33. In fact, Ms. Cousineau admits she ***authorized*** her phone to transmit location information, such as "when eating at a restaurant and 'checking in' with Facebook," Resp. 7:17, which would have resulted in Microsoft receiving anonymous location data. And discovery established Windows Phone 7 often resolves location requests on the phone itself ***without*** transmitting any data to Microsoft's servers, either to resolve the location request or to crowd source data. *See* Del Amo Casado Decl. [Dkt. 91] ¶¶ 9-10 (resolving location requests); 16-18 (crowdsourcing). As a result, Ms. Cousineau has no evidence her use of the Camera app—the only application alleged to have accessed location without her consent—ever caused transmission of location data to Microsoft.[1]

Unable to show Microsoft received any data without her consent, Ms. Cousineau claims Microsoft violated the SCA because it supposedly accessed communications Microsoft itself sent (i.e., location tiles sent by the Orion location service) after the tiles arrived at their destination (i.e., her phone). Specifically, she asserts Microsoft violated the SCA every time she opened her

[1] Although she no longer claims Microsoft unlawfully collected her location data, Ms. Cousineau asserts "a key merits issue" will be whether Microsoft made "intentional design decisions" to crowd source data without user consent. Resp. 5:26-27 & n. 4. In fact, uncontradicted evidence establishes the Camera team wrote the software to call for location immediately upon opening the application to maximize the software's ability to honor a user's decision whether to tag a photo and thereby "improve the user experience." Lydick Decl. [Dkt. 92] ¶ 2. Despite deposing five Microsoft employees, Ms. Cousineau cites nothing to support any contrary speculation—nor does she allege any other application had the same bug, as one would expect if the goal were to maximize crowd sourcing. In any event, the Camera app contributes only an insignificant amount of crowd sourced data. 3rd Del Amo Casado Decl. ¶ 12.

Camera app, because the Camera, a "software component loaded on the phone," would make a call "to another software component loaded on the phone (the location framework)," which checked location data on tiles previously sent to the phone by Microsoft and stored in RAM. *Id.* ¶ 5. Pretending Microsoft ***is*** its software for purposes of "access" under the SCA, Ms. Cousineau asserts Microsoft at that time "lacked … authority to access location information then in RAM"—even though Microsoft itself sent the communication containing that information. Resp. 7:14-15.

In any event, Microsoft did ***not*** access location data in RAM; rather, the software accessed the tiles. "Microsoft ***cannot*** access location information stored in RAM." Del Amo Casado Decl. [Dkt. 91] ¶ 21(d) (emphasis added). Ms. Cousineau offers no contrary evidence.

III. ARGUMENT

A. No Evidence Suggests Microsoft Accessed a Communication When the Location Framework Accessed Location Data in RAM.

To win at trial, Ms. Cousineau must show Microsoft accessed a "communication" it wasn't supposed to access. The statute imposes liability on "whoever … intentionally ***accesses*** without authorization a facility through which an electronic communication service is provided" or, if authorized to access such a facility, exceeds the authorization—and, ***in addition***, "obtains, alters, or prevents authorized access" to an electronic communication while in temporary storage. 18 U.S.C. § 2701(a) (emphasis added). "[T]he sort of trespasses to which the [SCA] applies are those in which the trespasser gains access to information to which he is not entitled to see." *Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr., Ltd.*, 965 F. Supp. 731, 740 (D. Md. 1997).

But ***Microsoft*** did none of this when the software on Ms. Cousineau's phone checked data on tiles sent by Microsoft's Orion service and then stored in RAM. Even if the phone were a facility under the SCA (which it is not), Ms. Cousineau presents no evidence suggesting ***Microsoft*** (a) "accessed" the phone when the location framework checked RAM or (b) obtained, altered, or prevented access to communications stored in RAM. Because Ms. Cousineau bears the burden of proof, her failure to produce evidence on these issues mandates summary judgment. *See Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986) (summary judgment proper if party with burden fails to "make a showing sufficient to establish the existence of an element essential to that party's case").

Further, the evidence ***negates*** liability: "Microsoft cannot access location information stored in RAM." Del Amo Casado Decl. [Dkt. 91] ¶ 21(d). The Court need go no further.

Ms. Cousineau largely argues around this issue rather than confronting it. She asserts Microsoft agreed users could limit its access to location data, and discusses crowdsourcing and data collection at length. *See* Resp. 18:16-19:10. But Ms. Cousineau no longer claims Microsoft engaged in unauthorized collection of data or crowdsourcing because—as explained above—she has no evidence it occurred without her consent. Instead, she alleges ***only*** the location framework on her phone accessed location data in RAM without authority. *See* Resp. 7:14-15, 18:10-11.

With respect to Microsoft's alleged access to RAM, Ms. Cousineau persists in arguing Microsoft faces punishing statutory damages, unrelated to actual harm, if "the ***software*** it programmed and distributed, rather than Microsoft itself, accessed Cousineau's RAM and the Beacon location information residing therein." Resp. 18:9-11 (emphasis added; quotation marks omitted). But Ms. Cousineau cites nothing to support this extraordinary proposition. She relies on cases where a defendant used software as a vehicle to facilitate ***actual access*** to communications. Thus, in *Miller v. Meyers,* 766 F. Supp. 2d 919, 923 (W.D. Ark. 2011), the defendant used "a keylogger program to obtain Plaintiff's passwords" and then "access[ed] Plaintiff's email account without authorization." In *Harris v. comScore, Inc.*, 292 F.R.D. 579, 582-83 (N.D. Ill. 2013), the defendant used software to intercept "phone numbers, social security numbers, user names, passwords, bank account numbers, credit card numbers, and other … information," and sold "the data collected from the consumer's computer." And in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 579-80 (1st Cir. 2001), a non-SCA case, the defendant used a "scraping" tool to collect data from a competitor's site, and it then used the data to compete. These cases all involve a defendant who used software as a tool to obtain what it never had the right to access.

Here, when the location framework component of the software on Ms. Cousineau's phone checked data in RAM on the phone, Microsoft itself neither accessed the device nor received information from it. Ms. Cousineau's expert concedes the point, Snead Dep. 38:11-22, 111:20-23, 113:7-14 [Dkt. 101 Ex. 1], and Microsoft's witness verifies it, Del Amo Casado Decl. [Dkt. 91]

¶ 21(d). Because the SCA makes a person liable only when that person "gains access to information … [it was] not entitled to see," *Educ. Testing Serv.*, 965 F. Supp. at 740, and Microsoft itself gained access to ***nothing*** in RAM, the Court should grant summary judgment.

B. Microsoft Accessed Only Information in RAM It Was Authorized to Access.

Even assuming Microsoft itself accessed RAM when the location framework checked for beacon data (which it did not), Ms. Cousineau concedes she "authorized Microsoft to access her location information on discrete occasions." Resp. 20:13-14. This concession disposes of Ms. Cousineau's claim: the SCA imposes liability ***only*** against a person who accesses a facility "without authorization" or "exceeds authorized access" to the facility. 18 U.S.C. § 2701(a).

Ms. Cousineau does not even argue Microsoft accessed a facility (under her mistaken theory, her phone) "without authorization." Access "without authorization" means access where a person has "***no rights***, limited or otherwise, to access the computer in question," *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (emphasis added),[2] and Ms. Cousineau admits she "authorized Microsoft to access" her phone for some applications. Instead, Ms. Cousineau argues Microsoft "exceeded authorized access" by checking information stored in RAM "when and where" she attempted to deny access by selecting "Cancel" when asked if she wanted the Camera app to tag her photos. Resp. 20:14-16. Her position is legally and factually incorrect.

First, courts hold "exceed[ing] authorized access" means accessing information the defendant is not permitted to access ***at all***—i.e., at any time, in any place, and for any purpose. *See, e.g.*, *Educ. Testing Serv.*, 965 F. Supp. at 740; *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 494-99 (D. Md. 2005); *cf. United States v. Nosal*, 676 F.3d 854, 856-57 (9th Cir. 2012) (interpreting "exceeds authorized access" in Computer Fraud and Abuse Act ("CFAA")). Courts reject Ms. Cousineau's assertion that this interpretation of the SCA would render the "prohibition on exceeding the scope of authorized access . . . meaningless." Resp. 22:1-4. In interpreting the same term in the CFAA, the Ninth Circuit explained "exceeds

[2] Although *Brekka* construed the meaning of "without authorization" under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Court cited *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2009), a case involving § 2701 of the SCA. The Ninth Circuit properly relied on *Theofel* because of the settled presumption Congress uses the same term consistently in different statutes. *See, e.g.*, *Smith v. City of Jackson, Miss.*, 544 U.S. 228, 233 (2005).

authorized access" refers to "someone who's authorized to access only certain data or files but accesses unauthorized data or files—which is colloquially known as 'hacking.'" *Nosal*, 676 F.3d at 856-57; *see id*. at 858 ("exceeds authorized access" applies to accessing "unauthorized information or files"). Thus, under the Ninth Circuit's interpretation—and Microsoft's—a person with a web-based email account such as Gmail or Hotmail could "exceed authorized access" to a facility through which that email service is provided by hacking into another person's account. The hacker is authorized to access the facility (i.e., the webmail provider's servers), so his access is not "without authorization." But by accessing information stored in the facility the hacker is not authorized to access at any time, he "exceeds authorized access." The operative language implements the statute's purpose of punishing hackers—but does not reach Microsoft here.

Second, even assuming Ms. Cousineau's Windows Phone 7 device is an SCA facility (it is not), Microsoft acted within its authority because it accessed only information it was entitled to access. *See* Resp. 21:25-27 & n.14 (admitting she authorized Microsoft to access location data in connection with Maps app). Ms. Cousineau argues Microsoft violated the SCA by allowing the Camera app to check tiles in RAM despite telling users they could prevent the Camera app from "us[ing] your location." She attempts to recast this non-actionable "misuse" theory as an "exceeds authorized access" claim, arguing Microsoft overstepped undefined limits on "when and where" it could access location information stored in RAM. Even assuming this theory could state an SCA claim (it cannot), Ms. Cousineau fails to present a genuine factual dispute as to whether any limits actually existed on the times or places when Microsoft was authorized to access RAM. Her opposition refers only to a limit on the Camera app's ability to ***use*** location information ("Allow the camera to ***use*** your location?"), Resp. 20:18-21 (citing Dkt. 65 ¶ 4) (emphasis added), and not to any limit on the software's ability to ***access*** at particular times and places tiles delivered by Microsoft and stored in RAM.[3] And Ms. Cousineau concedes she authorized Microsoft to access

[3] The Camera app did not "use" location against her wishes: it did ***not*** geotag pictures without user consent. Lydick Decl. [Dkt. 92] ¶ 2. Further, Ms. Cousineau states she permitted Microsoft to access data in RAM when she sought driving directions from the Maps app, but denied the Camera app's request to use location when she used her Camera app at work. *Id.* at 21:25-27 & n.14. But location settings in Windows Phone 7 and Microsoft apps do not provide users the ability to control the exact "time or place" when a Microsoft app uses location information. Rather, the controls gave users the ability to turn off location services altogether or to prevent individual apps from using location information, even though ***other*** apps can access the same information (unless the master switch is turned off). Even if

location information for other apps, such as Maps, without time or place limitations. *Id*. 21:25-27.

Because the SCA does not prohibit Microsoft from using information for any purpose that it is entitled to access for some purpose, Ms. Cousineau has no claim under the SCA.

C. Ms. Cousineau Fails to Distinguish the Growing Body of Case Law Holding Smartphones Are Not Facilities under the SCA.

Even if Ms. Cousineau offered evidence (which she has not) from which a jury could find Microsoft "exceeded authorized access" to communications when the Camera app called the location framework on the phone and the location framework accessed RAM to check data on location tiles, she still must also show Microsoft did so by accessing a "facility through which an electronic communications service ['ECS'] is provided." 18 U.S.C. § 2701(a). Ms. Cousineau concedes the case law since this Court decided Microsoft's Motion to Dismiss has uniformly held smartphones and PCs are not facilities under the SCA. *See* Motion [Dkt. 100] 13:24-14:11 & n. 4.

Facing this growing body of law, Ms. Cousineau purports to distinguish "each case cited" by Microsoft, claiming they deal with scenarios in which "the subject computer/phone [is] external to the ECS," which she says is not true of location services. Resp. 12:2-6. But Ms. Cousineau ignores *In re iPhone*, where the court found an Apple iPhone is not a "facility" through which Apple provides location services. Plaintiffs in *iPhone* made similar location-related allegations:

> Plaintiffs allege … Apple began intentionally collecting Plaintiffs' precise geographic location and storing that information on the iDevice in order to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States. … Apple represented that users could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iDevices to "off." Plaintiffs contend that Apple continued to monitor and store information about Plaintiffs' locations even when the functionality was disabled on users' iDevices.

In re iPhone App. Litig, 844 F. Supp. 2d at 1050-51 (citations omitted).[4] The *iPhone* court

the Camera app setting worked as she says it should, Ms. Cousineau's Camera app choice would not have limited Microsoft's ability to "access" the same location tiles for other apps. Her suggestion the bug in the Camera app prevented her from controlling "when and where" Microsoft could access location information is a red herring.

[4] The *iPhone* plaintiffs alleged more egregious conduct by Apple than Ms. Cousineau alleges here: they claimed Apple continued collecting location information even when the user turned off the master location services switch. (The iPhone handles location requests in similar fashion to a Windows Phone 7 device—including storing location information on the device "to improve the speed with which the iPhone can determine its own approximate location in response to future app requests." *In re iPhone App. Litig.*, N.D. Cal. No. 5:11-md-02250-LHK, Dkt. 235 (May 17, 2013) ¶¶ 4-7.) By contrast, Ms. Cousineau tacitly concedes she could have disabled location services, and precluded transmission of ***any*** location information, by switching off location services on her phone. Instead, she left location services switched "on," and she used location services from time to time. *See* Cousineau Decl. [Dkt. 72-26] ¶¶ 3-6.

dismissed the SCA claim because treating a phone as a "facility" for location services leads to anomalous results. *Id.* at 1058. Ms. Cousineau makes no effort to distinguish *iPhone*, and courts have cited it with approval on the SCA facility issue. *See Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012), *cert. denied*, 133 S. Ct. 2859 (2013); *Morgan v. Preston*, 2013 U.S. Dist. LEXIS 159641, *16 & n.3 (M.D. Tenn. 2013); *Roadlink Workforce Solutions L.L.C. v. Malpass*, 2013 U.S. Dist. LEXIS 133786, *9-*10 (W.D. Wash. 2013) (Leighton, J.).

Without mentioning *iPhone*, Ms. Cousineau makes a contorted effort to distinguish location services from other ECS. Ms. Cousineau claims in most cited cases (ignoring *iPhone*) "the subject computer/phone [is] external to the ECS itself" because an email or text message exists independent of the user's PC or smartphone: it resides on the ECS provider's servers, and the PC or smartphone merely allows the user to access the communication. Resp. 12:6-15. Ms. Cousineau asserts (without citing any support) location services are different. Without the Windows Phone 7 device, she says, location services communications never occur, since they depend on the phone's request for location information, and Orion's return of "tiled Beacon data" for "use[] by Location Framework." *Id.* 12:19-13:3. But Ms. Cousineau's argument amounts to nothing more than an immaterial observation: location services typically involve two-party communications between the user and the ECS provider (i.e., the device sends beacon information to the ECS, requesting location, and the provider responds), while text message and email services involve communications between a third party and a user, with the ECS's servers in the middle. But this makes no difference under the SCA. Whether the communication involves two or three parties, the smartphone or PC merely gives the user access to, or enables use of, the ECS; it is not the "facility" through which Microsoft provides the ECS to any ***other*** user, and that is dispositive.[5]

In other words, Ms. Cousineau's argument ignores the fundamental point: Microsoft's

[5] Ms. Cousineau also argues her phone is a "facility through which an electronic service is provided" because it may, under specific conditions, crowd source location data to Microsoft. Crowd sourcing anonymous data after some location requests allows an ECS provider to improve the accuracy of the location services it provides—but it does not provide the ECS itself. (Crowd sourced data is not the only source of information in location services databases. *See, e.g.*, Del Amo Casado Decl. [Dkt. 91] ¶ 21(a) (third-party database used by Apple); Deo Dep. [Dkt. 72-15] 101:1-14; 102:1-103:3 (third party database used to populate Orion).) Further, no court has held transmission of data from a PC or mobile device to a cloud-based communication service (e.g., Facebook) causes the PC or device to be a facility under the SCA. If it were, then nearly all PCs and devices would be "facilities"—and §2701(c)(1) of the SCA would allow those services to ***access*** those facilities—a result Congress could not have intended, given the SCA's purpose.

Orion servers communicate location data as a service to Windows Phone 7 users, such as Ms. Cousineau, as well as to other clients, such as Bing and Windows. *See* 3rd Del Amo Casado Decl. ¶ 11. And her phone enabled Ms. Cousineau to take advantage of location services Microsoft provided, i.e., to "use the device's location to [receive] improved services and experiences." Del Amo Casado Decl. [Dkt. 91] ¶ 3. But the phone did not enable ***other*** users to take advantage of Orion's services. Her "Windows Phone 7 device thus functions as the 'client' for location services provided by the GPS satellites and Orion." *Id.* ¶ 19. By contrast, if Orion ceased to exist, the location ECS would no longer function—because its servers, unlike the phone, ***are*** "facilities" providing an ECS to "clients" all over the world. The cases "consistently" hold a user's device "does not 'provide[] an electronic communication service' simply by virtue of enabling use of electronic communication services," which is all Ms. Cousineau's phone does. *In re iPhone*, 844 F. Supp. 2d at 1058 (citing *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001)); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, 2012 WL 3862209, *9 (S.D. Ohio 2012) ("facilities" protected by SCA "are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by [ECS] providers").

Finally, Ms. Cousineau ignores the absurd consequences of calling her device a facility. If the phone is a "facility through which an electronic service is provided," then section 2701(c)(1) of the SCA specifically allows the ECS provider (here, Microsoft) not only to access the phone itself—but ***also*** to grant third parties access. In other words, calling a personal device a facility expands dramatically the group with authorized access to the device under the SCA and thereby ***diminishes*** a user's privacy. To paraphrase *Crowley*: "It would … seem odd that the provider of a communication service [such as Microsoft] could grant access to one's [Windows Phone 7 device] to third parties, but that would be the result of [Ms. Cousineau's] argument." 166 F. Supp. 2d at 1271. Other cases, including one in this district, follow *Crowley* in finding it "illogical" to expand "facility" to reach personal devices on similar facts. *Roadlink*, 2013 U.S. Dist. LEXIS 133786, *9-*10 (Leighton, J.); *Lazette v. Kulmatycki*, 2013 WL 2455937, *16 (N.D. Ohio 2013); *Freedom Banc*, 2012 WL 3862209, *9; *In re iPhone*, 844 F. Supp. 2d at 1058.

Ms. Cousineau does not cite *Crowley*. And she tacitly admits if her phone were a "facility through which an electronic communication service is provided," the SCA would give Microsoft the right to access her phone—and to authorize ***others*** to access her phone. She shrugs off the concern as a consequence of "rapid technological advancement" Congress did not envision when it passed the SCA. Resp. 14:25-26 & n.8. But developments over the years have not changed the SCA's purpose: protecting the privacy of stored electronic communications. "[T]he words of a statute must be read in their context and with a view to their place in the overall statutory scheme," *Davis v. Mich. Dept. of Treasury*, 489 U.S. 803, 809 (1989), and a court must interpret a statute "as a symmetrical and coherent regulatory scheme." *Gustafson v. Alloyd Co*., 513 U.S. 561, 569 (1995). Ms. Cousineau fails to explain how ***expanding*** non-users' access to personal devices, such as her phone, furthers the statutory purpose. Plainly, as the courts have found, it does not.

On this record, the Court should join with courts across the country in holding the term "facility" under the SCA does not reach Ms. Cousineau's Windows Phone 7 device.

D. Location Information Stored in RAM Fails to Satisfy the SCA's Requirement of Storage "Incidental to" Transmission or for Backup.

Finally, Ms. Cousineau concedes she also has the burden of proving Microsoft obtained "access to … [an] electronic communication while it [was] in electronic storage," 18 U.S.C. § 2701(a), requiring her to show Microsoft accessed a communication while it was (a) in "temporary, intermediate storage … incidental to the electronic transmission thereof" or (b) in "storage … by an electronic communication service for purposes of backup protection." 18 U.S.C. § 2510(17). Ms. Cousineau contends Microsoft violated the statute when her phone's software accessed location tiles in RAM to check for data on beacons then "seen" by the device.[6] But Ms. Cousineau cannot satisfy either prong: the storage of tiles was neither (a) "intermediate" and "incidental to the electronic transmission thereof" nor (b) "for purposes of backup."

[6] Ms. Cousineau makes a confusing argument about whether "temporarily stored location information … fell between the Beacons themselves … and their endpoints" or "fell between Orion …, the WM7 device …, and Location Framework." Resp. 16:6-12. Leaving aside the inscrutability of Ms. Cousineau's references to where stored location information "falls," this case no longer involves access to transmissions by beacons or communications between the device and Orion. Further, even if communications of that nature ***were*** at issue, Ms. Cousineau offers no evidence suggesting Microsoft accessed them without her consent, and Microsoft is therefore entitled to summary judgment. *See Celotex Corp.*, 477 U.S. at 322. The ***only*** access in dispute relates to the location framework's query to determine if a location request can be resolved from data on tiles stored in RAM. The argument in the text focuses on that issue.

The references to "intermediate" storage "incidental to the electronic transmission thereof" reflect the SCA's purpose to "protect[] electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e., when an electronic communication service temporarily stores a communication while waiting to deliver it." *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); *see also Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part, vacated in part on other grounds*, 352 F.3d 107 (3d Cir. 2004) (same). Here, by the time the location framework "tries to resolve location through information located in [RAM] on the phone itself," Del Amo Casado Decl. [Dkt. 91] ¶ 10, the communication from Orion transmitting the tiles to RAM has been delivered—possibly days before. *See id.* ¶ 9. Ms. Cousineau has no evidence from which a jury could find her communications were accessed (by the software, not Microsoft) while in intermediate storage incidental to their transmission.

Hoping to sidestep the absence of evidence, Ms. Cousineau argues RAM in the abstract "is an intermediate storage medium that only temporarily holds data pending its ***movement elsewhere*** —such as to permanent storage (e.g. to flash storage), or being retrieved and utilized by software." Resp. 17:3-5 (emphasis added). But the SCA protects communications while in the midst of transmission from a sender to a recipient, using an ECS; nothing in the SCA evinces a purpose of protecting data residing in RAM on a personal device pending "movement elsewhere" on the device itself, accomplished ***without*** an ECS and accessed only by the user.[7] The SCA protects communications from a sender to a recipient through an ECS, which is not at issue here.

In any event, the record (which Ms. Cousineau ignores) shows the storage of tiles in RAM on a Windows Phone 7 device is not "incidental to the electronic transmission thereof." The tiles expire in ten days, even if not accessed, and then disappear. Del Amo Casado Decl. [Dkt. 91] ¶ 14. If the phone loads enough new tiles, the old ones roll off earlier. *Id.* And while in RAM, the data on the tiles may never be used: if the user moves outside the tiles' range before the next location request, the location framework will check the tiles, find "the tiles stored in RAM cannot

[7] Ms. Cousineau argues "electronic communications" encompass movement of data "***within the phone*** on wires and circuits." Resp. 9:14 (emphasis added). But she cites no authority holding the SCA protects data moving entirely within a device, such as a PC or a smartphone—and Microsoft knows of none. For one thing, software—not an ECS provider—enables transfers within a device, while the SCA reaches only communications through an ECS.

resolve the user's location," and the tiles become irrelevant to resolving the request. *Id.* ¶ 10. Thus, even assuming movement of tiles within the device could rise to the level of a transmission protected by the SCA (and it cannot), tiles in RAM are not in storage "incidental to the electronic transmission thereof" when the framework checks them to see if they contain relevant data.

That leaves Ms. Cousineau's footnote arguing location tiles are in temporary storage in RAM for "backup protection." Resp. 17:23-26 & n.11. "Backup protection" refers to retaining a ***copy*** of a communication for future use if, "for example, the message is accidentally erased from the user's own computer." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2003); *see Cheng v. Romo*, 2013 WL 6814691, *3 & n.3 (D. Mass. 2013) (emails in backup where, even after user downloaded emails, "the Yahoo! server continued to store copies"). Ms. Cousineau offers no ***evidence*** the tiles in RAM are back-ups of any communications. *See* Resp. 17:23 & n.11. In fact, the tiles contain data to use in resolving future location requests on the phone without a call to the Orion servers at Microsoft, even when the phone has no external data connection; they are not "backup." *See* 3rd Del Amo Casado Decl. ¶ 13 ("Microsoft does not 'back up tile data.'"); Del Amo Casado Decl. [Dkt. 91] ¶ 10. Further, Section 2510(17) of the SCA refers to backup storage "by an electronic communication service," ***not*** storage on a user's device. *Garcia*, 702 F.3d at 793 (storage "encompasses only the information that has been stored by an [ECS] provider"). Thus, Ms. Cousineau's cases, *Theofel*, 359 F.3d at 1071, and *Cheng*, 2013 WL 6814691, *3, each involved access to backup copies of emails stored with an ISP, not on the user's computer.

When the phone's location framework accesses data on tiles stored in RAM, it does not access a "communication" in "electronic storage," as the SCA uses those terms.

IV. CONCLUSION

Microsoft respectfully asks the Court to grant summary judgment dismissing Ms. Cousineau's SCA claim—the only claim remaining in the case.

DATED this 17th day of January, 2014.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Defendant Microsoft Corporation

By /s/ Stephen M. Rummage, WSBA 11168
Fred B. Burnside, WSBA #32491

Zana Bugaighis, WSBA #43614
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: (206) 622-3150, Fax: (206) 757-7700
E-mail: steverummage@dwt.com
E-mail: fredburnside@dwt.com
E-mail: zanabugaighis@dwt.com

CERTIFICATE OF SERVICE

I hereby certify that on January 17, 2014, the foregoing *Microsoft's Reply in Support of Motion for Summary Judgment* was electronically filed with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all counsel of record who receive CM/ECF notification, and that the remaining parties (if any) shall be served in accordance with the Federal Rules of Civil Procedure.

DATED this 17th day of January, 2014.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Defendant Microsoft Corporation

By *s/ Stephen M. Rummage*
Stephen M. Rummage, WSBA #11168
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: (206) 757-8136
Fax: (206) 757-7700
E-mail: steverummage@dwt.com